Horst-Görtz Institut
für IT Sicherheit

PRESENT

An Ultra-Lightweight Block Cipher

A. Bogdanov[1], L. R. Knudsen[3], G. Leander[1], C. Paar[1],
A. Poschmann[1], M. J. B. Robshaw[2], Y. Seurin[2], C. Vikkelsoe[3]

1 Ruhr-Universität Bochum
2 Technical University Denmark, Denmark
3 Orange Lab, France

CHES 2007

Outline

- Motivation
- PRESENT Specification
- Security Analysis
- Implementation Results
- Conclusion

Why yet another Block Cipher? (1)

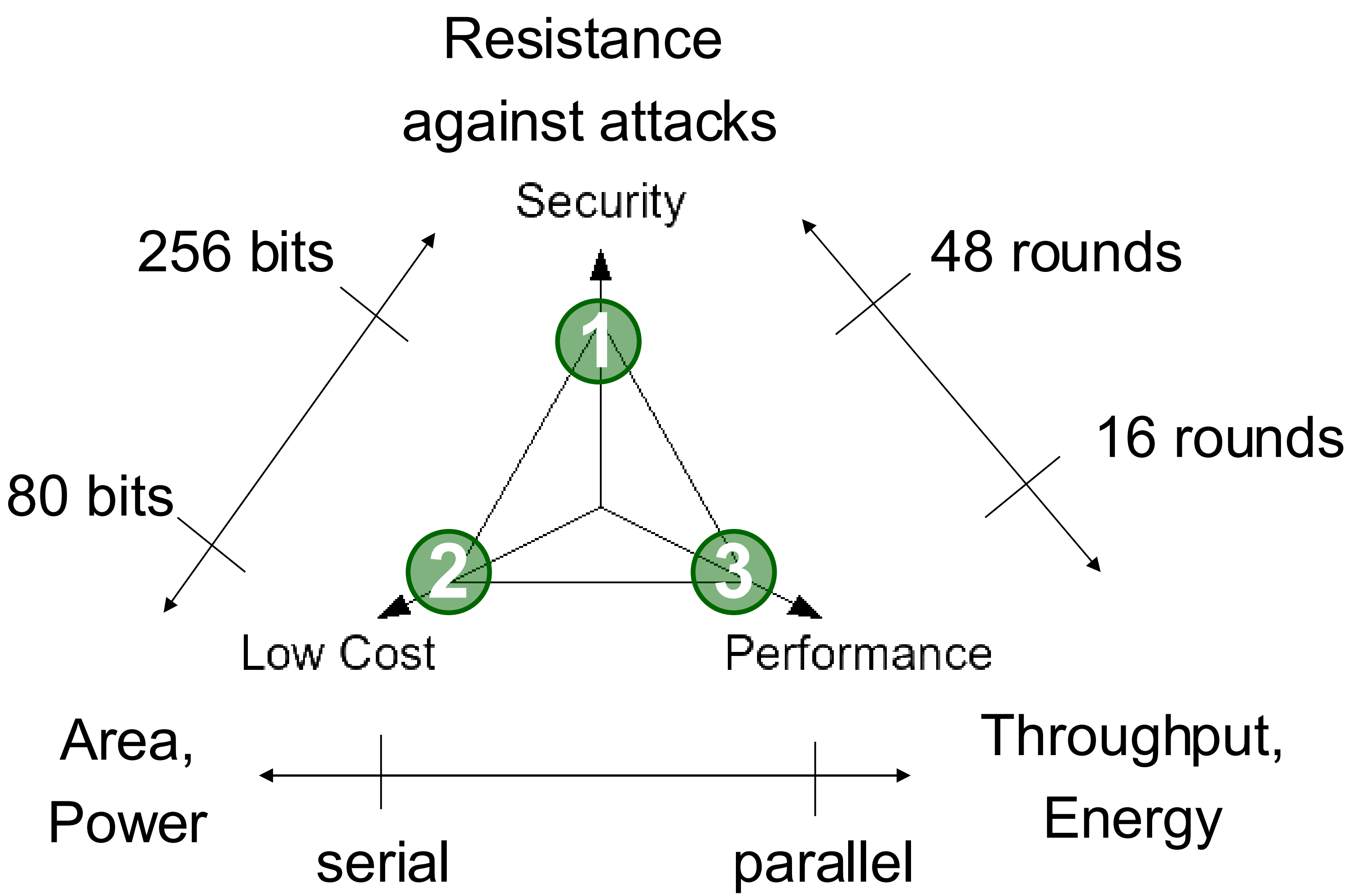
- Paradigm shift towards Pervasive Computing:
  - cost driven deployment
  - very constrained devices in terms of CPU, memory, power, and energy
  - small messages
- Traditionally efficient equivalent to high throughput
  - Known ciphers designed for high troughput, high speed, high …

→ Demand for an ultra-lightweight block cipher

Why yet another Block Cipher? (2)

- Security properties well understood
- Sound building blocks and design principles available
- Block ciphers can be used
  - as stream ciphers
  - for hashing

Metric and Tradeoffs



Requirements on PRESENT

Horst-Görtz Institut
für IT Sicherheit

- Design goals
  - Efficient hardware implementations
  - Moderate security level (80 bits)
  - Simplicity
- Small amounts of plaintexts
- encryption only core
- Metrics:
  1. Security
  2. Area, Power
  3. Speed

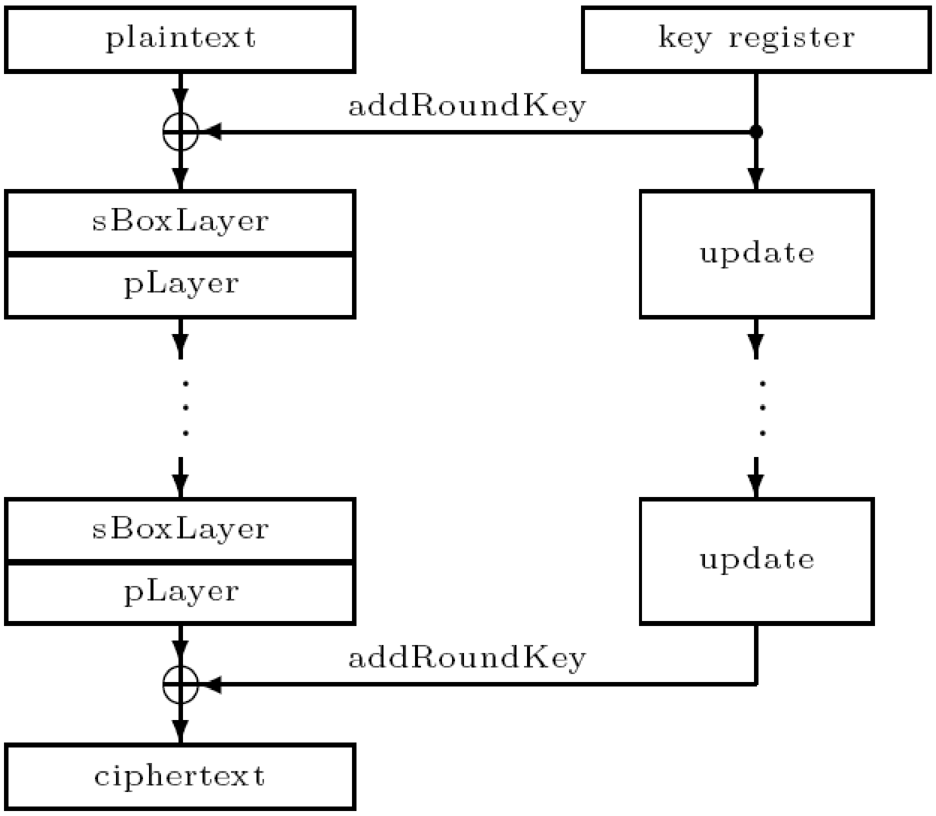
Outline

- Motivation
- PRESENT Specification
- Security Analysis
- Implementation Results
- Conclusion

Top Level Description of PRESENT

hgi
Horst-Görtz Institut
für IT Sicherheit

generateRoundKeys()
for $i = 1$ to 31 **do**
    addRoundKey(STATE,K_i)
    sBoxLayer(STATE)
    pLayer(STATE)
end for
addRoundKey(STATE,K_{32})



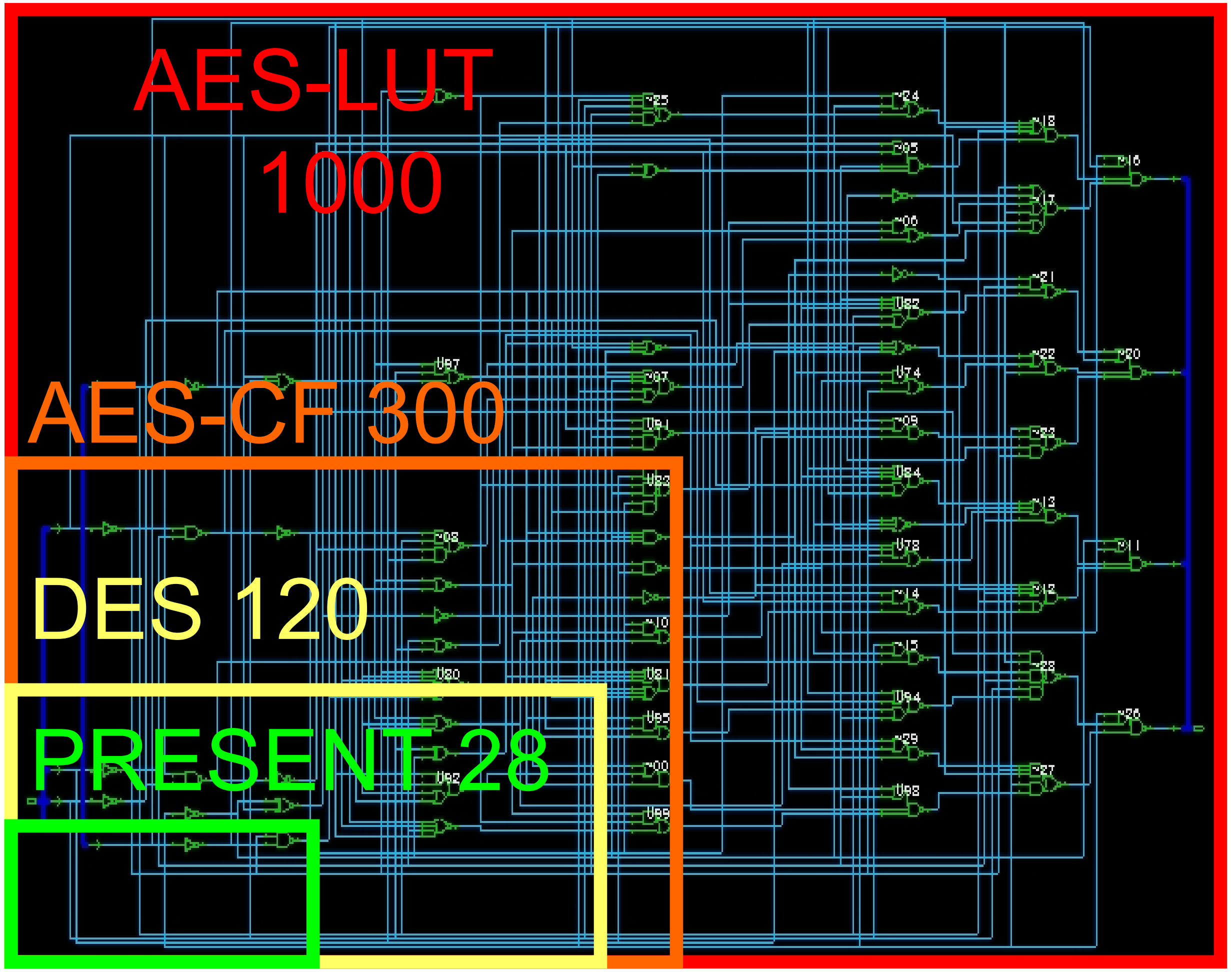
S-Boxes in Hardware

- LUT are realized as boolean functions
- Highly non-linear
- High boolean complexity
- Big area

8 x 8

6 x 4

4 x 4



S-Box Design Criteria

Horst-Görtz Institut
für IT Sicherheit

We denote the Fourier coefficient of S by

$$S_b^W(a) = \sum_{x \in \mathbb{F}_2^4} (-1)^{\langle b, S(x) \rangle + \langle a, x \rangle}.$$

1. For any fixed non-zero input difference $\Delta_I \in \mathbb{F}_2^4$ and any fixed non-zero output difference $\Delta_O \in \mathbb{F}_2^4$ we require

$$\#\{x \in \mathbb{F}_2^4 | S(x) + S(x + \Delta_I) = \Delta_O\} \leq 4.$$

2. For any fixed non-zero input difference $\Delta_I \in \mathbb{F}_2^4$ and any fixed output difference $\Delta_O \in \mathbb{F}_2^4$ such that $\mathrm{wt}(\Delta_I) = \mathrm{wt}(\Delta_O) = 1$ we have

$$\{x \in \mathbb{F}_2^4 | S(x) + S(x + \Delta_I) = \Delta_O\} = \emptyset.$$

3. For all non-zero $a \in \mathbb{F}_2^4$ and all non-zero $b \in \mathbb{F}_4$ it holds that $|S_b^W(a)| \leq 8$.
4. For all $a \in \mathbb{F}_2^4$ and all non-zero $b \in \mathbb{F}_4$ such that $\mathrm{wt}(a) = \mathrm{wt}(b) = 1$ it holds that $S_b^W(a) = \pm 4$.

PRESENT S-Box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

- Smallest 4x4 S-Boxes in hardware (28 GE)
- Fullfilling above conditions

PRESENT Permutation

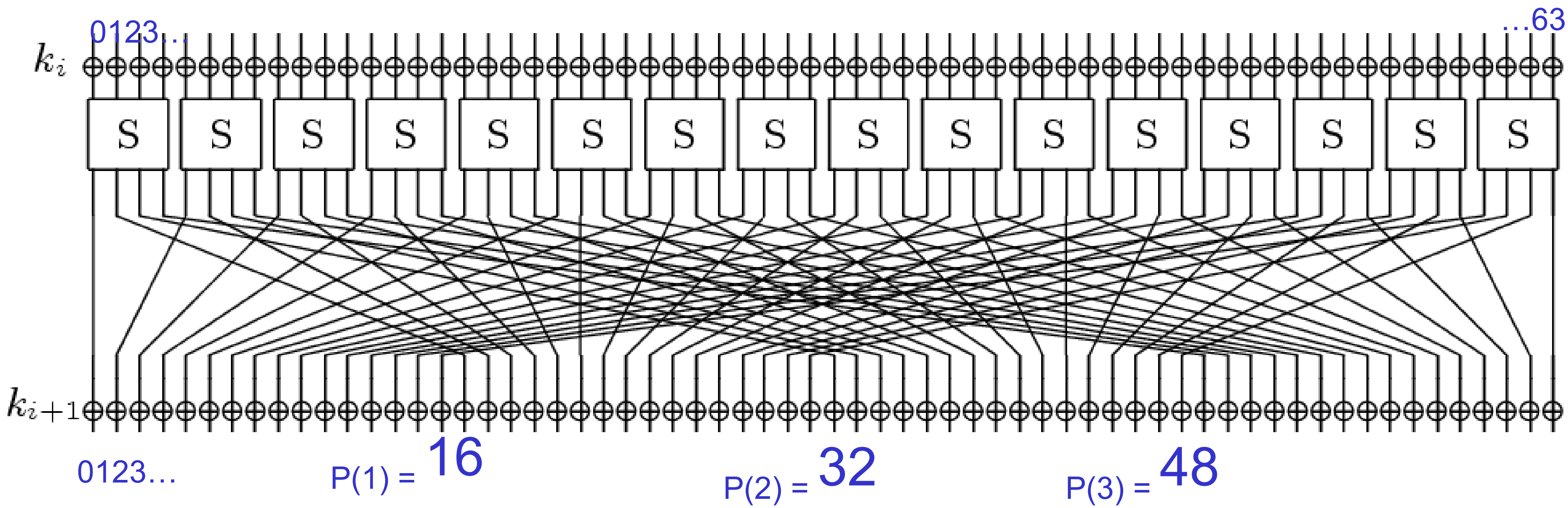
Horst-Görtz Institut
für IT Sicherheit

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P(i)$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

- Simple bit permutation

PRESENT Permutation - in Hardware

hgi
Horst-Görtz Institut
für IT Sicherheit



- Just wires
- No transistors required
- No delay

0 GE

(some wiring)

PRESENT Key Schedule

hgi
Horst-Görtz Institut
für IT Sicherheit

Notation:

- K 80-bit key register
- At round 1: $K = k_{79}k_{78}\ldots k_1k_0$ = initial key
- At round i: $K_i = k_{79}k_{78\ldots}k_1k_{16}$ = roundkey for round i

Updating K:

2. $[k_{79}k_{78}\ldots k_1k_0] = [k_{18}k_{17}\ldots k_{20}k_{19}]$
3. $[k_{79}k_{78}k_{77}k_{76}] = S[k_{79}k_{78}k_{77}k_{76}]$
4. $[k_{19}k_{18}k_{17}k_{16}k_{15}] = [k_{19}k_{18}k_{17}k_{16}k_{15}]$ XOR round_counter

Outline

- Motivation
- PRESENT Specification
- Security Analysis
- Implementation Results
- Conclusion

Differential Cryptanalysis

Theorem 1:

Any 5-round differential characteristic of PRESENT has at least 10 active S-Boxes.

- Any differential characteristic over 25 rounds must have at least 50 active S-Boxes
- Maximum differential characteristic is 2^{-2}
- Probability of 25-round characteristic is bounded by $(2^{-2})^{50} = 2^{-100}$

$2^{100} \gg 2^{64}$ (available PT/CT pairs)

$2^{100} \gg 2^{80}$ (key size)

Linear Cryptanalysis

Theorem 2:

Let ε_{4R} be the maximal bias of a linear approximation of four rounds of PRESENT. Then $\varepsilon_{4R} \leq 2^{-7}$.

- The maximum bias of a 28-round linear approximation is $2^6 \times (\varepsilon_{4R})^7 = 2^6 \times (2^{-7}) = 2^{-43}$
- About $(2^{43})^2 = 2^{86}$ known PT/CT pairs required

⇒

$2^{86} >> 2^{64}$ (available plaintext)

$2^{86} >> 2^{80}$ (key size)

Algebraic Cryptanalysis

- The PRESENT 4 x 4 S-Boxes can be described by 21 equations over GF(2) using 8 variables
  - 21x17x31 = 11,067 quadratic equations
  - 8x17x31 = 4,216 variables
- Small scale version analyzed
  - 7 S-Boxes
  - 28 bit block
  - 2 rounds

⇒ **Buchberger and F_4 algorithm fail to deliver a solution in a reasonable time for this 2-round 28-bit mini-PRESENT**

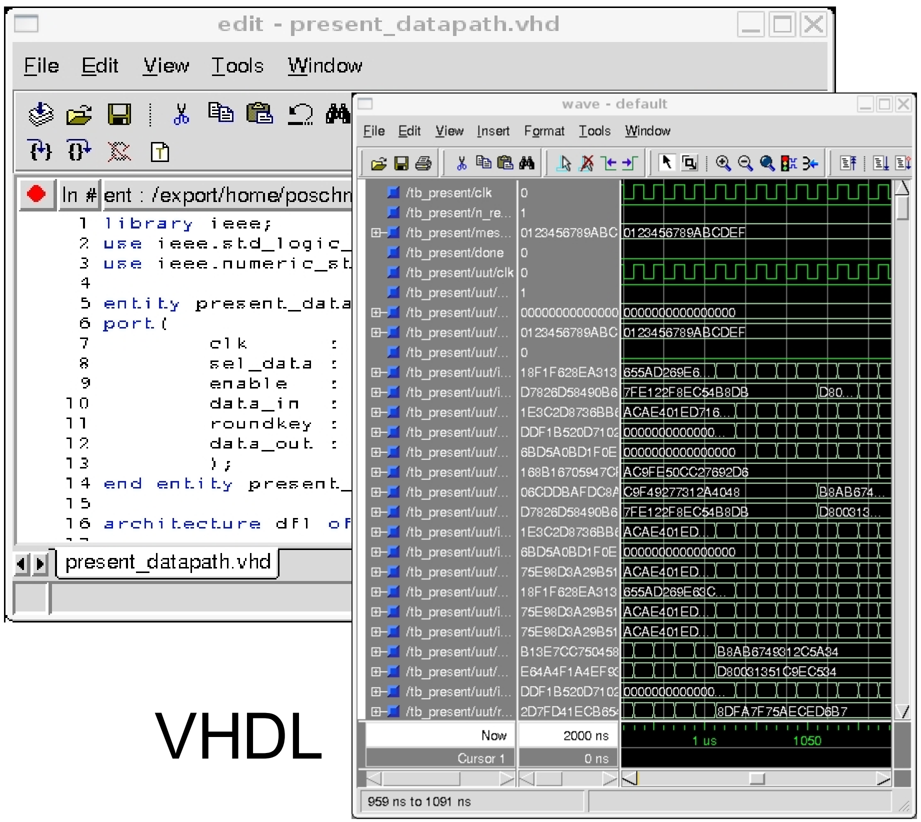
Outline

- Motivation
- PRESENT Specification
- Security Analysis
- Implementation Results
- Conclusion

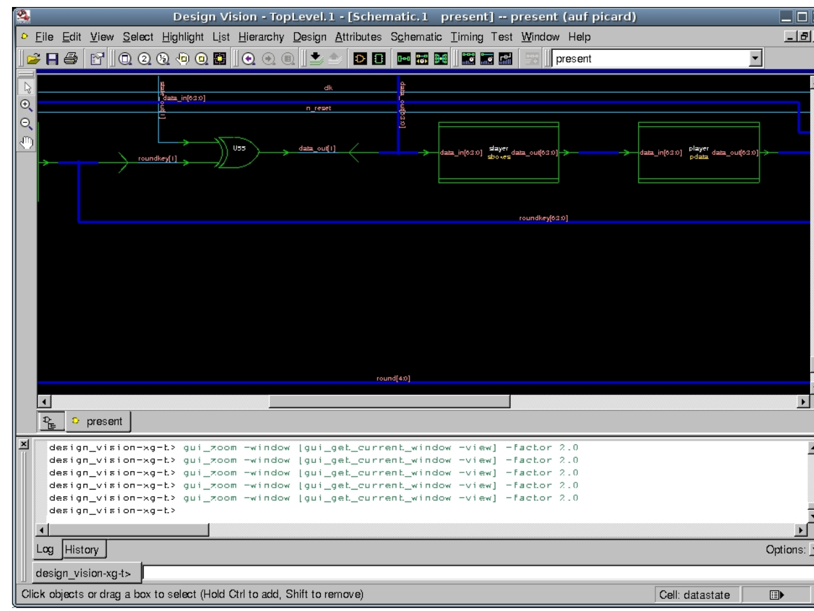
Toolchain

Mentor Graphics ModelSim SE Plus 5.8c

Synopsys DesignCompiler Y-2006-06



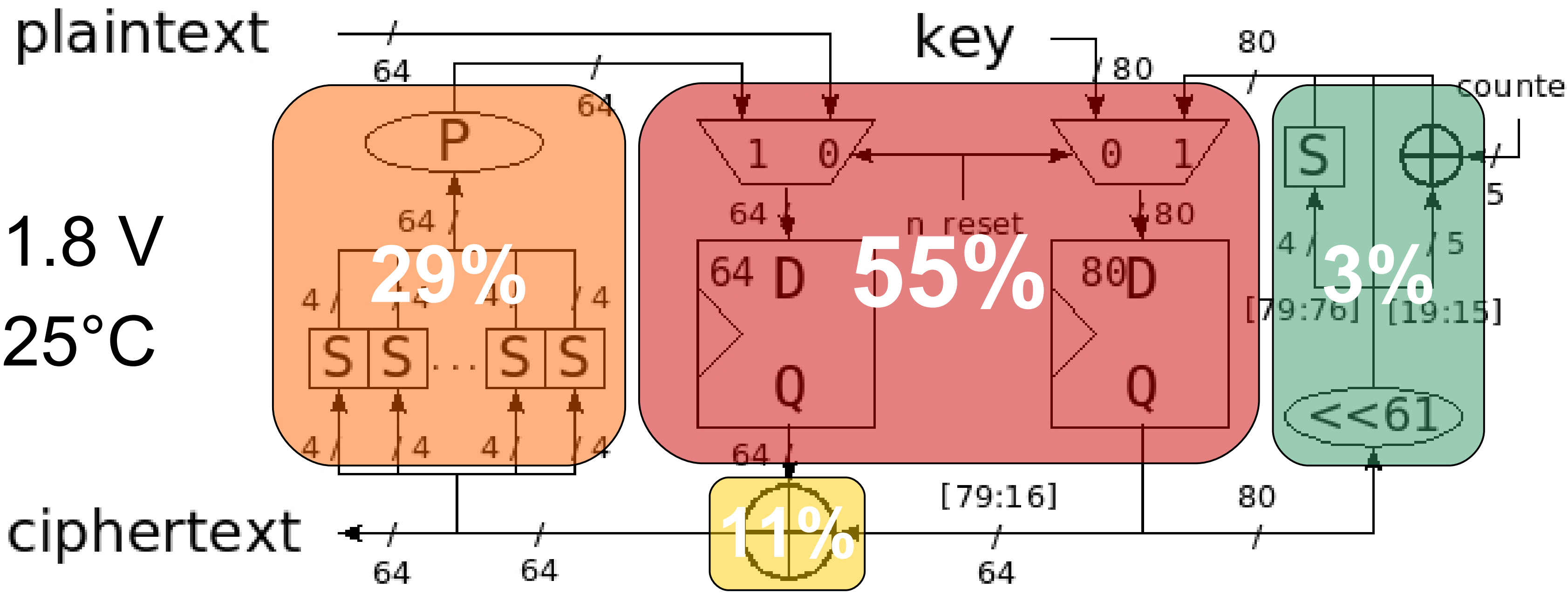
VHDL



Virtual Silicon UMCL18G212T3

PRESENT-80 Datapath

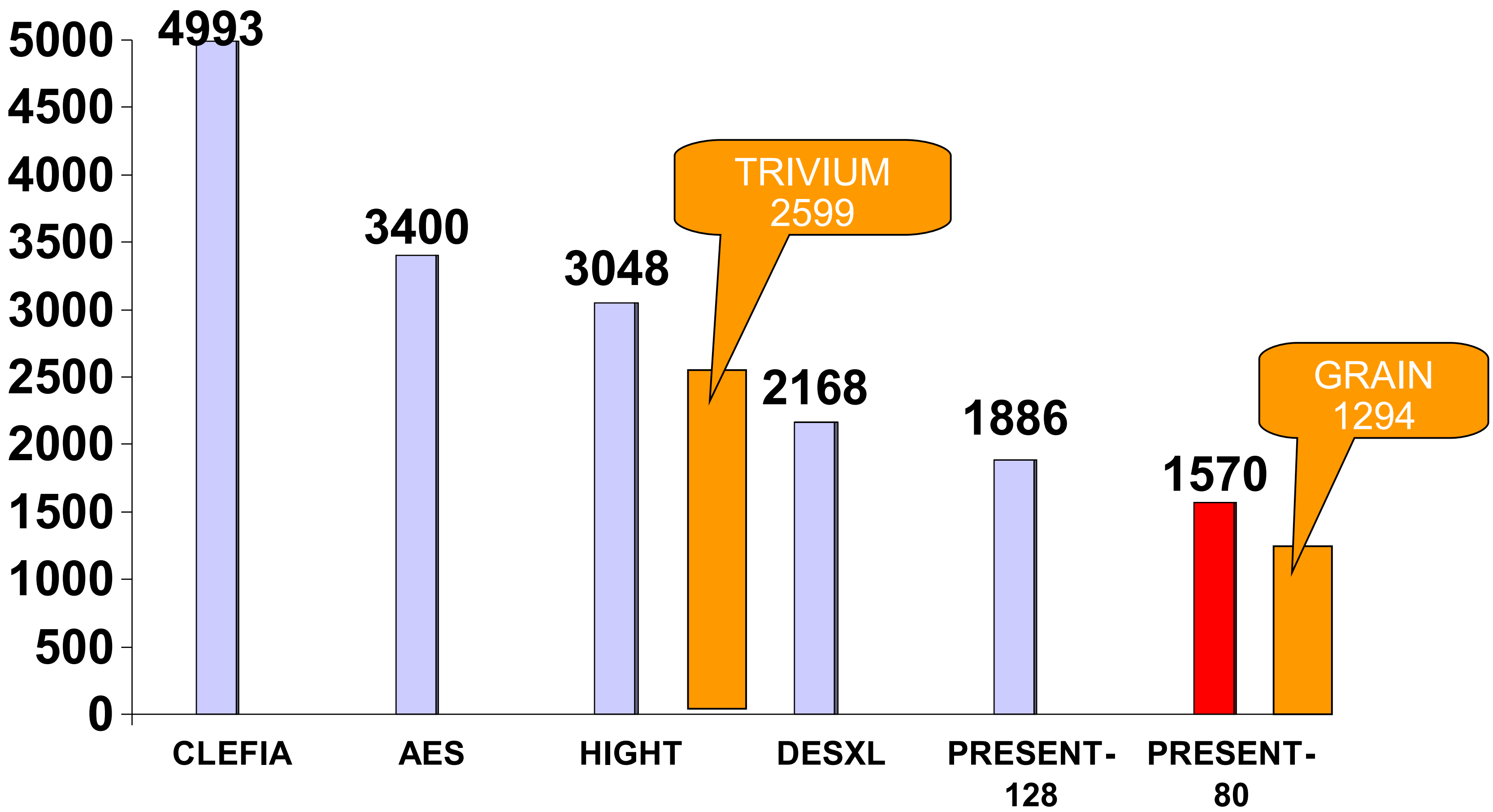
Horst-Görtz Institut
für IT Sicherheit



- 1.8 V
- 25°C

- 32 cycles
- 1570 GE
- 5 µW@100kHz

Comparison of Lightweight Ciphers



Outline

- Motivation
- PRESENT Specification
- Security Analysis
- Implementation Results
- Conclusion

Conclusion

- Presented the new block cipher PRESENT
- SPN with 64-bit state, 80-bit key, 31 rounds
- Based on well-known design principles (feature)
- Very small footprint in hardware (1570 GE)
- Low power estimates (5 µW)
- Lightweight block ciphers have similar footprint as stream ciphers

Please try to break PRESENT!

Horst-Görtz Institut für IT Sicherheit

Thank you!

Questions?

www.crypto.rub.de

poschmann@crypto.rub.de

PRESENT Permutation - Further Notes

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51

$$P(i) = \begin{cases} 16 * i \bmod 63, & 1 \leq i \leq 62 \\ i, & i \in \{0,63\} \end{cases}$$

- Involution P(P(P(i))) = i
- Could be useful for serialization